مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة تدقيق أمن المعلومات			
النسخة:	١,٠			
التصنيف:	◉ عامة	○ سرية	○ سرية عالية	○ سرية للغاية
الحالة:	معتمده	**النوع :**	وثيقة	
تاريخ الإصدار:	٢٠١٥/٠٦/٢٥			
تاريخ المراجعة:	٢٠١٥/٠٦/٢٥			

النسخة رقم	التاريخ	إعداد ومراجعة	الملاحظات
١,٠	٢٠١٥/٠٦/٢٥	الإدارة العامة لتقنية المعلومات (قسم أمن المعلومات)	النسخة الأولى من الوثيقة

الموظف المختص

النسخة رقم	التاريخ	المختص	الملاحظات
١,٠	٢٠١٥/٠٦/٢٥	محمد الشهري	تم المراجعة

الإعتماد

النسخة رقم	التاريخ	المعتمد/ المعتمدين	الملاحظات
١,٠	٢٠١٥/٠٧/٠٨	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد	

جدول المحتويات

١. تعريف هيكلة السياسة

تشتمل وثيقة السياسة على العناصر التالية:

- **الهدف:** وصف مختصر لأغراض وأهداف السياسة.
- **نطاق العمل:** تحدد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.
- **الإمتثال والتنفيذ:** تحدد تبعات ونتائج أية مخالفة لهذه الساسة.
- **السياسات:** يشتمل هذا القسم على وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.

٢. الهدف

الغرض من هذه السياسة هو التأكد من قيام جامعة الملك خالد بتخطيط وتنفيذ مراجعات وعمليات تدقيق مستقلة لأمن المعلومات المتعلقة بأنظمتها المعلوماتية بما يتوافق مع خطورة وحساسية تلك الأنظمة، ومن ثم اتخاذ الإجراءات لمعالجة الملاحظات التي تم استخلاصها من عملية المراجعة والتدقيق.

٣. نطاق العمل

تطبق هذه السياسة على جميع الموظفين، والموردين، وشركاء العمل، والموظفين المتعاقدين، والوحدات الوظيفية لدى جامعة الملك خالد سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم. كما تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٤. الإمتثال و التنفيذ

في حالة مخالفة أي موظف أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لدى جامعة الملك خالد لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر- نظام العمل والعمال، ونظام مكافحة الجرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٥. **السياسات** :

- **تخطيط وتنفيذ عمليات تدقيق ومراجعة أنظمة المعلومات بناءً على المخاطر**

- يجب أن تقوم جامعة الملك خالد بتقييم حالة ضوابط أمن المعلومات لديها من خلال إجراء تدقيق ومراجعة لأمن المعلومات الخاصة بأنظمة المعلومات وذلك بناءً على تقييم المخاطر، ويتم تخطيط تدقيق أنظمة المعلومات بناءً على درجات التصنيف المحددة لأمن المعلومات لدى الجامعة (عامة، سرية، سرية عالية، سرية للغاية). يتم تحديد جميع المنشآت المادية لدى الجامعة وتعيين تصنيف أمني لها.
- يجب أن تستخدم الجامعة المبادئ التالية عند تخطيط تدقيق أمن المعلومات لأنظمة المعلومات لديها:
  - أنظمة المعلومات التي أعطيت تصنيفاً للمخاطر بدرجة سرية للغاية، يتم تدقيقها بشكل نصف سنوي كحد أدنى.
  - أنظمة المعلومات التي أعطيت تصنيفاً للمخاطر بدرجة سرية عالية، يتم تدقيقها مرة واحدة سنوياً كحد أدنى.
  - أنظمة المعلومات التي أعطيت تصنيفاً للمخاطر بدرجة سرية، يتم تدقيقها مرة واحدة كل سنتين.
  - أنظمة المعلومات التي أعطيت تصنيفاً للمخاطر بدرجة عامة، يتم تدقيقها سنوياً.
- يجب أن يتم تطوير برامج التقييم التفصيلي مع الأخذ في الاعتبار الضوابط المعيارية المحددة لأمن النظام والمتطلبات الأمنية الأخرى وأفضل الممارسات في هذا الصدد حسبما ينطبق على أنظمة المعلومات.
- يجب أن تجري الجامعة تدقيقاً رسمياً على أنظمة المعلومات التي لديها.
- يجب أن يتم إجراء التدقيق على أنظمة المعلومات بعناية، وبمعرفة المسؤولين عن أنظمة المعلومات، بحيث يتم الحد من مخاطر الإزعاج والإيقاف لخدمات/ عمليات النشاط.
- يجب أن يكون الشخص/ الأشخاص الذين يقومون بإجراء عمليات التدقيق مستقلين عن الأنشطة التي يقدمونها.
- يجب أن تستخدم الجامعة موارد داخلية وخارجية مستقلة لإجراء التدقيقات على أنظمة المعلومات لديها.
- يجب على جميع موظفي الجامعة والمتعاقدين الآخرين أن يبدوا التعاون الكامل أثناء تدقيق أنظمة المعلومات.

- **مسؤولية اتخاذ الإجراءات التصحيحية بالوقت المناسب**

- يكون المسؤولون عن أنظمة المعلومات والراعين لها مسؤولين عن اتخاذ الإجراء التصحيحي المناسب لمعالجة نتائج التدقيق.
- يجب أن تقوم إدارة الجامعة بمتابعة الأشخاص المسؤولين للتأكد من معالجة نتائج التدقيق بسرعة و بشكل فاعل.

- **حماية الأدلة التي تظهر أثناء التدقيق**

- يجب على المدقق التأكد من دعم نتائج تدقيق أنظمة المعلومات بالأدلة والقرائن.
- يجب على المدقق التأكد من اتخاذ خطوات كافية لحماية سلامة ونزاهة الأدلة التي تم جمعها أثناء التدقيق، ومثال ذلك، وضع الأدلة في ملفات وحفظها في مكان آمن، والوصول المصرح به لملف أدلة المراجعة.

- **التحكم في استخدام أدوات تدقيق أنظمة المعلومات**

- يجب على الجامعة أن تتأكد من استخدام أدوات تدقيق أنظمة المعلومات المصرح بها فقط في سياق عملية التدقيق، وعليها اتخاذ التدابير اللازمة نحو ما يلي:
  - منع إساءة سوء الاستخدام المحتمل لأدوات تدقيق الأنظمة (ومثال ذلك استخلاص معلومات سرية دون تفويض مناسب).
  - التأكد من الحفاظ على سلامة ونزاهة أنظمة المعلومات والبيانات المتعلقة بها.
  - تفادي الخلل والتوقف المحتمل لأنظمة المعلومات نتيجة استخدام تلك الأدوات.